DETAILED ACTION

This office action is response to the proposed amendment on August 1, 2011 in which claims 1-11, 19-27, 29-30, 32, and 34 are presented for examination. Claims 12-18, 28, 31, 33, and 35-36 have been cancelled. Claims 1, 19, 26, 30, 32, and 34 have been amended.

Information Disclosure Statement

The information disclosure statement filed on 3/6/2006 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because the documents are undated. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided

by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with applicant's representative John M. Carson, on August 1, 2011.

Amendment to the Claims

2. CLAIMS:

Please replace the claims below as follows:

1. (Currently Amended) A data processing system for distributing and authenticating documents, ~~from a plurality of parties to a recipient data processing apparatus~~, the data processing system comprising

a plurality of document distribution devices each configured to generate an original hash value ~~from the content of~~ based on an electronic file containing a document to be distributed, wherein the document distribution devices collectively generate a plurality of original hash values; and

a data communications network configured to communicate each of the original hash values to the recipient data processing apparatus before a predetermined event, the recipient data processing apparatus comprising a processor configured to generate hash values, the recipient data processing apparatus configured to:

receive the original hash values from each of the plurality of document distribution devices via the data communication network,

generate an original super hash value from the plurality of the original hash values received, and

communicate the original super hash to the plurality of document distribution devices,

wherein after the predetermined event, the plurality of document distribution devices are configured to:

communicate each of the ~~respective~~ electronic files to the recipient data processing apparatus,

wherein the recipient data processing apparatus is further configured to:

generate a comparative hash value ~~from the content of~~ based on the electronic file containing the document received from each of the document distribution devices,

generate a comparative super hash value from each of the comparative hash values,

communicate the comparative super hash value to each of the document distribution devices, and

determine whether or not each of the documents of the electronic files received ~~by the recipient data processing apparatus~~ from the document distribution devices have changed from a comparison of at least one of the original hash values and the comparative hash values, and the comparative super hash value and the original super hash value.

12-18. (Canceled)

19. (Currently Amended) A recipient data processing device configured to authenticate documents received from ~~one or more~~ a plurality of document distribution devices via a data communications network, the recipient data processing device comprising:

a communications interface configured to receive a plurality of original hash values from the document distribution devices via the data communication network before a predetermined event, wherein the hash values are each generated based on an electronic file containing one of the documents; and

a data processing apparatus comprising a ~~hashing~~ processor configured to generate an original super hash value from the plurality of the received original hash values, and communicate the original super hash value to each of the document

distribution devices, wherein the data processing apparatus is configured to operate in combination with the communications interface to:

receive, after the predetermined event, ~~respective~~ a plurality of electronic files from the document distribution devices, each of the electronic files containing one of the documents,

generate a comparative hash value ~~from the content of~~ based on the electronic file ~~containing the document~~ received from each of the document distribution devices,

generate, using the ~~hashing~~ processor, a comparative super hash value from each of the comparative hash values,

communicate the comparative super hash value to the document distribution devices, and

determine whether or not each of the documents of the electronic files received ~~by the recipient data processing apparatus~~ from the document distribution devices have changed based on a comparison of at least one of the original hash values and the comparative hash values, and the comparative super hash value and the original super hash value.

26. (Currently Amended) A computer-implemented method for distributing documents, the computer-implemented method comprising: ~~from a plurality of parties to a recipient data processing apparatus, the method comprising:~~

~~generating, for each of the plurality of parties, an~~ generating a plurality of original hash values, each ~~from the content of~~ original hash value based on one of a plurality of ~~an~~ electronic files, each file representing a document to be distributed;

communicating the original hash values to the recipient data processing apparatus before a predetermined event via a data communications network;

generating, at the recipient data processing apparatus, an original super hash value ~~from~~ based on the plurality of the original hash values; ~~received;~~

communicating the original super hash value to ~~the~~ a plurality of document distribution devices; and, after the predetermined event,

communicating, from the plurality of document distribution devices, each of the ~~respective~~ electronic files representing a document to the recipient data processing apparatus;

generating, at the recipient data processing apparatus, a comparative hash value ~~from the content of~~ based on the electronic files representing ~~containing~~ the documents received from ~~each of~~ the document distribution devices;

generating a comparative super hash value from each of the comparative hash values; and

determining whether or not each of the documents of the electronic files received ~~by the recipient data processing apparatus~~ from the document distribution devices have changed based on a comparison of at least one of the original hash values and the comparative hash values, and the comparative super hash value and the original super hash value.

28. (Canceled)

30. (Currently Amended) A method of authenticating documents received from a plurality of document distribution devices via a data communication~~s~~ network, the method comprising:

receiving a plurality of original hash values from the document distribution devices, before a predetermined event, via the data communication network, each original hash value based on one of a plurality of electronic files, each file containing a document to be distributed;

generating an original super hash value from the plurality of the original hash values received;

communicating the original super hash value to each of the document distribution devices;

receiving, after the predetermined event, ~~respective~~ a plurality of electronic files from the document distribution devices, each received electronic file;

generating a comparative hash value from the content of based on the received electronic files; containing the document received from each of the distribution devices;

generating a comparative super hash value from each of the comparative hash values;

communicating the comparative super hash value to the document distribution devices; and

determining whether or not each of the documents of the received electronic files ~~received by the recipient data processing apparatus~~ from the document distribution devices have changed based on a comparison of at least one of the original hash values, and the comparative hash value and the comparative super hash value and the original super hash value.

31. (Canceled)

32. (Currently Amended) A non-transitory computer readable medium having a program for executing a method of authenticating documents received from a plurality of document distribution devices via a data communications network, the method comprising:

receiving a plurality of original hash values from the document distribution devices, before a predetermined event, via the data communication network, each original hash value based on one of a plurality of electronic files, each electronic file containing a document to be distributed;

generating an original super hash value from the plurality of the original hash values received;

communicating the original super hash value to each of the document distribution devices;

receiving, after the predetermined event, ~~respective~~ the plurality of electronic files from the document distribution devices;

generating a comparative hash value from the content of based on the received electronic files; containing the document received from each of the distribution devices;

generating a comparative super hash value from each of the comparative hash values;

communicating the comparative super hash value to the document distribution devices; and

determining whether or not each of the documents of the received electronic files ~~received by the recipient data processing apparatus~~ from the document distribution devices have changed based on a comparison of at least one of the original hash values, and the comparative hash value and the comparative super hash value and the original super hash value.

33. (Canceled)

34. (Currently Amended) A data processing apparatus for distributing documents from a plurality of ~~parties~~ document distribution devices to a recipient data processing apparatus, the data processing apparatus comprising:

means for generating, for each of the plurality of ~~parties~~ document distribution devices, ~~an~~ a plurality of original hash values, ~~from the content of~~ each original hash value based on one of a plurality of ~~an~~ electronic files, each file representing a document to be distributed;

means for communicating the original hash values to the recipient data processing apparatus, before a predetermined event, via a data communications network;

means for generating, at the recipient data processing apparatus, an original super hash value ~~from the~~ based on the plurality of ~~the~~ original hash values; ~~received;~~

means for communicating the original super hash to the plurality of document distribution devices;

means for communicating, after the predetermined event, from the plurality of document distribution devices, each of the ~~respective~~ electronic files representing a document to the recipient data processing apparatus;

means for generating, after the predetermined event, at the recipient data processing apparatus, a comparative hash value ~~from the content of~~ based on the electronic files representing ~~containing~~ the documents received from ~~each of~~ the document distribution devices;

means for generating, after the predetermined event, a comparative super hash value from each of the comparative hash values; and

means for determining whether or not each of the documents of the electronic files received ~~by the recipient data processing apparatus~~ from the document distribution devices have changed based on a comparison of at least one of the original hash values and the comparative hash values, and the comparative super hash value and the original super hash value.

35-36. (Canceled)

Allowable Subject Matter

3. Claims 1-11, 19-27, 29-30, 32, and 34 are allowed.

Reasons for Allowance

4. The following is an examiner's statement of reasons for allowance:

As to amended independent claims 1, 19, 26, 30, 32, and 34, the prior art of records (US 2003/0159048 A1 to Matsumoto and Patent No. US 7,117,367 B2 to Carro) alone or in combination fail to anticipate or render obvious the claimed features.

Matsumoto (prior art of record) discloses stamping system for electronic documents where the software for document preparation is integrated with the time stamping function, so that everyone can easily treat authenticated time data, and a user

can select himself or herself an easy verification method or a difficult and strict verification method for verifying a time stamp according to the importance of a document to be verified (Paragraph 0047: The electronic document preparing organization 20 fetches time data from the center each time a time stamp processing request is generated, and transmits a digest value (hash value)for a document to be time-stamped to the center each time the time stamp processing is performed, while the center assigns time data and an electronic signature to the digest value and returns the digest value to the organization).

The reference of Carro (prior art of record) teaches authenticating a text document with links to a plurality of files by modifying at least a selected attribute of invisible characters on a plurality of inter-word intervals of the text document where a one-way hash function of each file is computed in order to obtain a hash value composed of a subset of hash digits for each one (Col 8 lines 27-29: computing a one-way hash function of each file of the plurality of files to obtain a hash value composed of a subset of hash digits for each file; Col. 10 lines 41-46: computing a one-way hash function of each of the files in order to obtain a new hash value for each one; and means for comparing the new hash value to an origin hash value for each file n of the N files with n being 1 to N in order to authenticate a file n).

Applicant's argument filed on 07/13/2011, see page 13-14, is persuasive as the combination of prior art references fails to teach the claimed invention and falls into impermissible hindsight reconstruction of applicant's claims at the time the applicant's

invention was made (04/11/2003) because of the non-obvious claimed limitations. For example, Claim 1 recites:

"…a data communications network configured to communicate each of the original hash values to the recipient data processing apparatus before a predetermined event…wherein after the predetermined event, the plurality of document distribution devices are configured to:…

generate a comparative super hash value from each of the comparative hash values,

communicate the comparative super hash value to each of the document distribution devices, and

determine whether or not each of the documents of the electronic files received from the document distribution devices have changed from a comparison of at least one of the original hash values and the comparative hash values, and the comparative super hash value and the original super hash value…."

wherein the invention discloses that an original hash value is communicated to a recipient data processing apparatus before a predetermined event and the electronic document is communicated to the recipient data processing apparatus after the predetermined event where it is determined whether or not each of the documents of the electronic files received from the document distribution devices have changed from a comparison of at least one of the original hash values and the comparative hash values, and the comparative super hash value and the original super hash value (See, Paragraph 0011).

None of the prior art of records, either taken by itself or in any combination, would have anticipated or made obvious determining whether or not each of the documents of the electronic files received from the document distribution devices have changed from a comparison of at least one of the original hash values and the comparative hash values, and the comparative super hash value and the original super hash value at or before the time the application was filed.

Claims 2-11 are also allowed by virtue of their dependency on the base claim 1.

Claims 19, 26, 30, 32, and 34 and its dependent claims 20-25, 27, and 29 recite similar features as in claim 1 and its corresponding dependent claims and thus, Claims 19-27, 29-30, 32, and 34 are allowed for the same reason stated above for claim 1.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MAHFUZUR RAHMAN whose telephone number is (571)270-7638. The examiner can normally be reached on Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571) - 272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R./

Examiner, Art Unit 2438

/Taghi T. Arani/

Supervisory Patent Examiner, Art Unit 2438